DCS3101
Assignment 3

Kent Odde

October 28, 2020

Contents

Abstract

This is my submission for the third compulsory assignment in DCS3101, Introduction to Cybersecurity.

Q1

> *What are the advantages of firewalls?*

A firewall is a component, that functions as a check-point in a network, and its job is to monitor and regulate traffic passing through it.

The main use case and advantage of a firewall, is that we can protect a local trusted network against threats which might exist on another untrusted network.

When implemented, all traffic passing from network A to network B must pass through the firewall. The firewall may prohibit traffic it considers a threat. This decision has traditionally been based on a predefined ruleset, but next-generation firewalls have much more sophisticated methods of identifying potential threats.

A strength of firewalls is their wide range of types suitable for different needs, and their capability for configuration. We can have an open firewall, where we define rules for what the firewall should filter out, or for a more conservative approach, we can have a firewall which filters all packages, and we whitelist the traffic we do want.

We can filter traffic based the sender or receiver or by the contents of the packets, which can be used to protect specific hosts or specific ports. We can filter based on the types of application layer protocol the package contains, which can help us filter out spam mail etc. We can also use the TCP headers, so that an outgoing TCP packet on a port, will temporarily open the port for incoming packets, given that the TCP header contain the correct information.

There are also *next-generation* firewalls, which can employ machine learning to be able to recognize unknown types of malicous traffic based on patterns.

As an added bonus of all this, we can also configure firewalls to log all traffic, which may be very handy for several reasons, but especially if we find out that our network has been compromised.

Q2

Comment if the following is true or false in the context of TLS - "The algorithms inside a session are negotiated between client and server." Justify your answer with an associated protocol diagram.

The statement in the question is **true**. Different clients and servers will have support for different encryption and MAC algorithms. Just like different people speak different languages. The goal of the negotiation is to find mutually supported algorithms, that are also recognized as secure enough by the current version of TLS.

However, negotiation is perhaps a strong word. If we look at subset of the TLS handshake protocol in figure 1, we can see that the client starts the conversation with a *hello*.

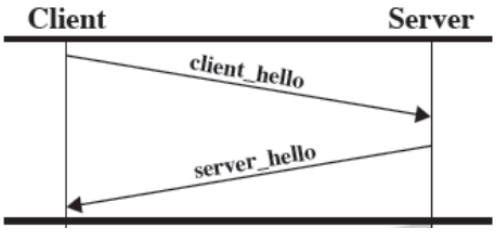

Figure 1: Part of the TLS handshake protocol diagram from lecture

This hello consists of information about the client, like what algorithms it has support for. One of the things the server then does, is to pick the strongest of these algorithms that it self supports. The server hello will then among other things, contain this decision.

Q3

> *It was discussed in the class about one particular attack on TLS. Discuss this attack and identify another attack that can impact TLS. Discuss briefly about the attack you have chosen for your answer.*

The attack discussed in class was the exploitation of what has come to be known as the *heartbleed bug*. This was a bug in the heartbeat protocol of TLS.

The heartbeat protocol, is a mechanism for letting the client check that the connection with the server is still active. The client would send a message asking for a distinct string as a reply, and the character length of this string. If the connection was still alive, the server would naturally send the requested string back.

However, it was discoverd that if the number containing the length of the string was much higher than the actual length of the string, the server would in addition to the string send random content of its RAM. This was of course catastrophic, as a web-servers RAM is filled with a lot of information that can be exploited, like encryption keys and so on.

Q4

What are the differences between IDS and IPS? Discuss on classification/taxonomy of IDS and IPS.

Q5

Biometrics - What are the key factors for choosing a biometric modality (e.g., face, fingerprint, iris, etc)?

Q6

What kind of attacks are possible on face biometric systems?

Appendices

References

[1] English Letter Frequency, cornell university. http://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html. Accessed: Sept-20.